IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	10/067,610
Confirm. No.:	5884
Inventor:	Rafie Shamsaasef et al.
Filing Date:	February 4, 2002
Title:	Method and System for Providing Third Party Authentication of Authorization
Examiner:	Okoronkwo, Chinwendu C.
Art Unit:	2136
Atty. Docket No.:	D02684

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

This document is filed in response to the Notice of Non-Compliant Appeal Brief mailed from the U.S. Patent and Trademark Office on November 12, 2008. No fee is believed to be due. This document replaces the Appeal Brief filed on October 16, 2008.

Please enter this as an Appeal to the Examiner's Final Rejection mailed from the U.S. Patent and Trademark Office on November 16, 2007. The Notice of Appeal was filed on May 16, 2008.

(I) Real Party in Interest

General Instrument Corporation, a wholly owned subsidiary of Motorola, Inc., is the real party in interest.

(II) Related Appeals and Interferences

There are no related appeals or interferences known to the Applicant.

(III) Status of Claims

Claims 1, 3, 5-15, and 17-20 are pending and presently stand twice and finally rejected and constitute the subject matter of this appeal.

Claims 1 and 5 stand rejected under 35 U.S.C. § 102(e) as being allegedly anticipated by U.S. Publication Number 2003/0018913 to Brezak et al. (hereinafter "Brezak").

Claims 3, 6-15, and 17-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Brezak and further in view of U.S. Pat. No. 6,381,331 B1 to Kato (hereinafter "Kato").

Claims 2, 4, and 16 have been canceled.

Applicant appeals all pending claims 1, 3, 5-15, and 17-20.

(IV) Status of Amendments

Applicant did not submit any After Final amendments in response to the Final Rejection mailed from the U.S. Patent and Trademark Office on November 16, 2007.

Applicant's most recent amendment to the claims was submitted on March 16, 2007, together with a Request for Continued Examination. The claims as thus amended are included in Appendix A attached hereto.

(V) Summary of Claimed Subject Matter

Embodiments of the present invention concern a method, such as that recited by claim 1, for communication authorization. A third party server receives a request for access information to access content. *See, e.g.*, page 12,. lines 1-10; page 18, lines 18-25; page 19, lines 1-21. The access information and session rights to access the desired content from a first application server are generated. *See, e.g.*, page 20, lines 4-13. Authentication is generated for the access information and session rights, using a first service ticket to the first application server. *See, e.g.*, page 20, lines 4-13; page 21, lines 16-25; page 22, lines 1-4. The first service ticket is obtained from a key distribution center (KDC). *See, e.g.*, page 11, lines 1-10. The access information, session rights and authentication are sent to a client, *see, e.g.*, page 27, lines 6-21, page 28, lines 13-21, whereby the client presents the access information, session rights and authentication to the first application server to be authorized to receive the desired content from the first application server. *See, e.g.*, page 30, lines 1-7.

Other embodiments of the present invention concern a method, such as that recited by claim 8, for verifying authorization for a client to gain access to content and/or services. A key request is received from a client. *See, e.g.*, page 12, lines 20-21; page 27, lines 6-21; page 28, lines 22-25; page 29, lines 1-8. Third party server access information, session rights and third party server authentication are extracted from the

key request, and verification is done for an authentication of the third party access information, session rights and a client authorization. *See, e.g.*, page 24, line 10 to page 26, line 14. A key reply is issued if the authentication of the third party access information, session rights and the client authorization are verified. *See, e.g.*, page 26, lines 15-25; page 27, lines 1-6. The KDC receives a second service ticket request from a client for the application server, and a second service ticket for the application server is issued. *See, e.g.*, page 22, lines 12-24. In the step where the application server receives a key request from a client, the key request includes the second service ticket. *See, e.g.*, page 22, lines 12-24.

Further embodiments of the present invention concern a method, such as that recited by claim 17, for providing secure communication when distributing services. A third party server receives a selection for services. *See, e.g.*, page 12, lines 1-10; page 18, lines 18-25; page 19, lines 1-21. Access information and session rights for the services are issued. *See, e.g.*, page 18, lines 18-25; page 19, lines 1-6. Authentication of the access information and the session rights is issued. *See, e.g.*, page 12, lines 11-19; page 18, lines 18-25; page 19, lines 1-6; page 21, lines 16-25; page 22, lines 1-4. An application server receives a key request from a client. *See, e.g.*, page 12, lines 20-21; page 27, lines 6-21; page 28, lines 22-25; page 29, lines 1-8. The method verifies an authentication of the access information, session rights and a client authorization utilizing, at least in part, a first service ticket. *See, e.g.*, page 24, line 10 to page 26, line 14. A key reply is issued to a client if the authentication of the access information, session rights and the client authorization are verified. *See, e.g.*, page 26, lines 15-25; page 27, lines 1-6.

(VI) Grounds of Rejection to be Reviewed on Appeal

Whether the rejection of claims 1 and 5 under 35 U.S.C. § 102(e) as being anticipated by Brezak is proper.

Whether the rejection of claims 3, 6-15, and 17-20 under 35 U.S.C. § 103(a) as being unpatentable over Brezak and further in view of Kato is proper.

(VII) Argument

Rejections under 35 U.S.C. §101

None.

Rejections under 35 U.S.C. §112, first paragraph

None.

Rejections under 35 U.S.C. §112, second paragraph

None.

Rejections under 35 U.S.C. §102

Claims 1 and 5

The rejections of claims 1 and 5 under 35 U.S.C. § 102(e) are respectfully traversed.

The Examiner relies on Brezak as the primary reference in continuing to reject the claims. Brezak is a different system than that presently claimed by Applicant. Brezak allows a first server to be a proxy for the client when requesting data from a second server. *See* paragraphs [0044], [0046], [0048] and [0054]. By way of being a proxy,

server 210 forwards client specific information directly to another server such as server 212 or 214. *Id.*

As can be seen in Applicant's Fig. 1, neither server 107 nor 106 acts as a proxy for client 102 to request data from the other. The claims, as presently written, support this contention. Specifically, claim 1 includes the language

> sending the access information, session rights and authentication to a client, whereby the client presents the access information, session rights and authentication to the first application server to be authorized to receive the desired content from the first application server

As can be seen from this language, it is the client (and not another server as described in Brezak) that forwards information to the data-providing server.

In making the present rejection, the Examiner equates the claimed "third party server" with Brezak's trusted third-party server 206. Brezak also gives examples of what the trusted third-party server 206 could be, and Brezak's examples include being a key distribution center (KDC). See paragraph page 12, lines 20-21. Therefore, the Examiner is equating the claimed "third party server" with a KDC. This interpretation conflicts with Applicant's claim language because later in claim 1, Applicant recites a KDC as a separate entity from the third party server. Thus, equating Brezak's trusted third-party server 206 with Applicant's claimed "third party server" renders Applicant's later recitation of a "key distribution center" out of the claim and this is improper.

In response to this argument, the Examiner asserts in the Final Rejection that the claim language "does not distinguish the KDC as being a separate entity." Applicant disagrees. The claim clearly recites a "third party server" and a "KDC." If Applicant had

intended for the KDC to be the "third party server," Applicant would have claimed the third party server instead of the KDC. The Examiner is re-writing the claims in an effort to make an inappropriate reference apply to the present application. While Applicant agrees that the specification cannot be read into the claims, the Examiner cannot similarly read out express limitations from a claim in order to make a rejection.

The Examiner also asserts that Brezak teaches "sending the access information, session rights and authentication to a client," in paragraph [0048][1]. Brezak does not transmit any information to the client in paragraph [0048]. Instead, Brezak teaches sending client information from trusted third-party server 206 to server 210. The client 202 receives nothing in paragraph [0048]. Indeed, since the purpose of Brezak is to have one server act as a proxy for a client, as previously described, the client would never send this type of information because that responsibility has been delegated to a server.

Applicant notes that an authentication reply is sent to a client in paragraph [0042]. However, no mention of access information or session rights is made in Brezak's paragraphs [0039] - [0043]. Thus, Brezak does not teach all of the limitations of claim 1 as asserted by the Examiner.

Claims 5 is allowable at least because claim 5 depends from independent base claim 1, which is an allowable base claim for at least the reasons discussed above.

Rejections under 35 U.S.C. §103

Claims 3, 6-15, and 17-20

[1] In the response to arguments, the Examiner cites to paragraphs [0039]-[0043]. However, the rejection on page 5 of the Final Rejection cites to paragraph [0048].

The rejections of claims 3, 6-15, and 17-20 under 35 U.S.C. § 103(a) are respectfully traversed.

Claims 3, 6, and 7 are allowable at least because claims 3, 6, and 7 depend from independent base claim 1, which is an allowable base claim for at least the reasons discussed above with respect to the rejection of claim 1 under § 102(e).

With respect to independent claims 8 and 17, Applicants respectfully submit that the Examiner relies on alleged teachings in the Brezak reference that, in fact, are not disclosed or suggested by Brezak, and are not supplied by Kato.

First, the Examiner asserts with respect to claims 8 and 17 (at pages 12 and 20, respectively, of the final Office Action) that Brezak teaches "issuing a key reply" in paragraph [0048]. Applicants respectfully submit that the Examiner is incorrect, in that Brezak does not disclose issuing a key reply. Applicant's claim 17 further includes the limitation that the key reply is issued to a client:

> issuing a key reply **to a client** if the authentication of the access information, session rights and the client authorization are verified

(emphasis added). This feature is not taught by Brezak. Indeed, Brezak does not transmit any information to the client in paragraph [0048]. Instead, Brezak teaches sending client information from trusted third-party server 206 to server 210. The client 202 receives nothing in paragraph [0048].

Applicant's claim 8 further includes the limitation that the key request is received from a client:

> the application server receiving a key request **from a client** wherein the key request includes the second service ticket

(emphasis added). The Examiner cites paragraph [0045] for this feature; however, this limitation is absent from Brezak. The messages 230 and 232 in Figure 2 of Brezak are between the server A 210 and the trusted third party 204 and do **not** involve a message from a client.

Indeed, since the purpose of Brezak is to have one server act as a proxy for a client, as previously described, the client would never send this type of information because that responsibility has been delegated to a server. Brezak does not present any data to the first application server that controls content distribution. Instead, Brezak passes service credential data from either the client or from another source on behalf of the client to a server that then obtains desired content from the target server. Paragraph [0008]. Thus, as has been previously stated, a server asks for content on behalf of the client in Brezak as opposed to the present application where the client asks for the content directly from the server controlling access to the content.

It would be contrary to this teaching of Brezak to have "the application server receiving a key request from a client," as required by claim 8, and "issuing a key reply to a client," as required by claim 17. "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be . . . led in a direction divergent from the path that was taken by the applicant." *In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 2006) (quoting *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994)). Thus, Brezak *teaches away* from "the application server receiving a key request from a client" and *teaches away* from "issuing a key reply to a client."

Even if Brezak were combined with Kato, or other prior art references, Applicant respectfully submits that Brezak fails to provide a basis for a rejection under 35 U.S.C. §

103, at least because Brezak expressly *teaches away* from either "the application server receiving a key request from a client" or "issuing a key reply to a client." Because Brezak is an improper basis for rejecting Applicant's claims, the combination of Brezak with Kato, or other prior art references, also is an improper basis for rejecting Applicant's claims.

Kato fails to supply the foregoing features missing from Brezak, and accordingly, the combination of Brezak and Kato cannot suggest the invention and cannot render the claims obvious. Thus, no matter how Brezak and Kato may be combined (even assuming, arguendo, that one of ordinary skill in the art would be led to combine them) the resulting combination is not the invention recited in any of independent claims 1, 8, and 17. Dependent claims 3, 6, and 7 which depend on claim 1 and incorporate all of the limitations thereof are similarly patentable. Dependent claims 9-15 which depend on claim 8 and incorporate all of the limitations thereof are similarly patentable. Likewise, dependent claims 18-20 which depend on claim 17 and incorporate all of the limitations thereof are similarly patentable.

Accordingly, Applicants respectfully request withdrawal of the rejection of claims 3, 6-15, and 17-20 under 35 U.S.C. § 103(a).

(VIII) Claims Appendix

A copy of the currently pending claims is attached.

(IX) Evidence Appendix

No additional evidence is provided in an evidence appendix.

(X) Related Proceedings Appendix

No related proceedings are provided in a related proceedings appendix.

Respectfully submitted,

RAFIE SHAMSAASEF, et al.

Date: November 12, 2008

BY: /Stewart M. Wiener/
Stewart M. Wiener
Registration No. 46,201
Attorney for Applicants

MOTOROLA, INC.
101 Tournament Drive
Horsham, PA 19044
Telephone: (215) 323-1811
Fax: (215) 323-1300

CLAIMS APPENDIX

1. (Previously presented) A communication authorization method, comprising:

a third party server receiving a request for access information to access content;

generating the access information and session rights to access the desired content from a first application server;

generating authentication of the access information and session rights using a first service ticket to the first application server, wherein the first service ticket is obtained from a key distribution center (KDC); and

sending the access information, session rights and authentication to a client, whereby the client presents the access information, session rights and authentication to the first application server to be authorized to receive the desired content from the first application server.

2. (Canceled)

3. (Previously presented) The method as claimed in claim 1, further comprising:

encrypting at least a portion of the session rights using a third party server session key for the first application server.

4. (Canceled)

5. (Previously presented) The method as claimed in claim 1, further comprising:

requesting a ticket granting ticket (TGT ticket);

receiving a TGT ticket;

requesting the first party server service ticket for the first application server; and

receiving the first party server service ticket for the first application server.

6. (Previously presented) The method as claimed in claim 1, further comprising:

the first application server receiving a key request including the access information and authentication;

extracting the access information and authentication;

verifying the authentication of the access information using the first service ticket, and client authorization;

issuing a key reply if the authentication of the access information and client authorization are verified;

the KDC receiving a second service ticket request from a client for the application server;

issuing a second service ticket for the application server; and

the step of the application server receiving a key request from a client wherein the key request includes the second service ticket.

7. (Previously presented) The method as claimed in claim 6, further comprising:

a client generating a key request including the access information and the authentication;

sending the key request to the first application server; and

receiving the key reply (KEY_REP) if the authentication of the access information and client authorization are verified by the first application server.

8. (Previously presented) A method for verifying authorization for a client to gain access to content and/or services, comprising:

receiving a key request from a client;

extracting third party server access information, session rights and third party server authentication from the key request;

verifying an authentication of the third party access information, session rights and a client authorization;

issuing a key reply if the authentication of the third party access information, session rights and the client authorization are verified;

the KDC receiving a second service ticket request from a client for the application server;

issuing a second service ticket for the application server; and

the step of the application server receiving a key request from a client wherein the key request includes the second service ticket.

9. (Previously presented) The method as claimed in claim 8, further comprising:

authenticating the third party server access information using the third party server authentication.

10. (Previously presented) The method as claimed in claim 9, wherein the authenticating includes extracting a first service ticket and authenticating the third party server access information using the first service ticket.

11. (Previously presented) The method as claimed in claim 8, wherein the extracting the third party server authentication, further comprising the steps of extracting a session key from the first party ticket included in the key request; and the step of authenticating the access information includes verifying a third party server signature using the session key.

12. (Previously presented) The method as claimed in claim 11, wherein the extracting the session key includes decrypting at least a portion of the first party ticket included in the key request using the first application server service key and extracting the session key.

13. (Previously presented) The method as claimed in claim 5, further comprising:

the third party server receiving a request for the access information to access content;

generating the third party server access information to access the desired content from a first application server; and

generating the third party server authentication of the access information.

14. (Previously presented) The method as claimed in claim 13, wherein the generating the third party server authentication includes incorporating a first party server service ticket for the first application server.

15. (Previously presented) The method as claimed in claim 14, wherein the generating the authentication includes generating a signature utilizing a session key of the first party server service ticket.

16. (Canceled)

17. (Previously presented) A method for providing secure communication when distributing services, comprising:

a third party server receiving a selection for services;

issuing access information and session rights for the services;

issuing authentication of the access information and the session rights;

an application server receiving a key request from a client;

verifying an authentication of the access information, session rights and a client authorization utilizing, at least in part, a first service ticket; and

issuing a key reply to a client if the authentication of the access information, session rights and the client authorization are verified.

18. (Previously presented) The method as claimed in claim 17, further comprising:

a KDC receiving a first service ticket request from a third party server for the first application server;

the KDC issuing the first service ticket to the third party server for the first application server; and

the steps of the third party server issuing access information and authentication including generating the access information and authentication using the first service ticket.

19. (Previously presented) The method as claimed in claim 17, further comprising:

the KDC receiving a second service ticket request from a client for the first application server;

issuing a second service ticket for the first application server; and

the step of the application server receiving a key request from a client wherein the key request includes the second service ticket.

20. (Previously presented) The method as claimed in claim 17, wherein: the verifying the authentication of the access information includes:

extracting the first service ticket;

decrypting the first service ticket;

extracting a session key from the first service ticket;

generating a signature using the session key; and

verifying the signature over the access information with the session key.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.